REMARKS

Introduction

In the November 10, 2004 Office Action, claim 10 was objected to under 37 C.F.R. §1.75(c) as being of improper dependent form. Claims 1-3, 5-9, 11-17, 19-22, and 24 were rejected under 35 U.S.C. §103(a) as being unpatentable over so-called Applicant's Admitted Prior Art (AAPA) in view of Mont (the Time Vault article), Smith (U.S. patent 6,061,448), and Lee (U.S. Pub. No. 20020188690). Claim 4 was rejected under 35 U.S.C. §103(a) as being unpatentable over AAPA in view of Mont, Smith, Lee, and Boneh (U.S. Pub. No. 20030081785). Claim 10 was rejected under 35 U.S.C. §103(a) as being unpatentable over AAPA in view of Mont, Smith, Lee, and McMorris (U.S. Pub. No. 20030163567). Claim 18 was rejected under 35 U.S.C. §103(a) as being unpatentable over AAPA in view of Mont, Smith, Lee, and "Mont2" (U.S. Pub. No. 20030198348). Claim 23 was rejected under 35 U.S.C. §103(a) as being unpatentable over AAPA in view of Mont, Smith, Lee, and Martija (U.S. Pub. No. 20020169857). These rejections are respectfully traversed.

The Objection to Claim 10

Claim 10 was objected to under 37 C.F.R. §1.75(c) as being of improper dependent form. According to 37 C.F.R.

§1.75(c), one or more claims may be presented in a patent application in dependent form, referring back to and further limiting another claim or claims in the same application. Claim 10 is in accordance with 37 C.F.R. §1.75(c), because it refers back to claim 7 and further limits claim 7. In particular, claim 10 further limits claim 7 by adding another required method step. The additional method step added by claim 10 is the step of "providing the certificate that contains the service name of the IBE public parameter information host to the sender ..." The method step of claim 10 is not present in claim 7 (or in claim 1 from which claim 7 depends), so the method step of claim 10 "further limits" claims 1 and 7 as required by 37 C.F.R. 1.75(c). Claim 10 is therefore in proper form and the objection to claim 10 should be withdrawn.

The Prior Art Rejection of Claims 1-24

Applicants' invention is related to secure messaging systems. In particular, the invention relates to messaging arrangements that use identity-based-encryption (IBE) techniques.

In IBE encryption systems, a message recipient's email address or other identity-based information may be used as the basis for the recipient's IBE public key, so it is generally not necessary to look up a given recipient's public key as with

conventional public-key-encryption systems such as the RSA system. Recipients of IBE-encrypted messages use corresponding IBE private keys to decrypt the messages.

Although a sender of a message in an IBE system generally need not look up a recipient's public key before sending an encrypted message to a recipient, the sender must obtain IBE public parameter information that is associated with the recipient prior to encrypting the message. This general characteristic of IBE systems is described in the background section of the present patent application (the section referred to as "AAPA" in the Office Action).

In an environment in which different groups of recipients each have a different set of IBE public parameter information, it becomes critical for a sender to obtain a copy of the appropriate set of IBE public parameter information for a desired recipient. If the sender is not able to obtain the correct IBE public parameter information, the sender cannot use IBE encryption to encrypt a message for the desired recipient.

As described in applicants' specification (e.g., on page 3, line 18 to page 5, line 8), applicants' invention provides a solution to this problem. In particular, applicants disclose an arrangement in which each set of IBE public parameter information is stored on a corresponding IBE public parameter host. Each public parameter host has a service name.

A sender who desires to send an encrypted message to a given recipient may use the recipient's IBE public key and a service name generation rule to determine which IBE public parameter host should be contacted to obtain the appropriate IBE public parameter information for that given recipient. The sender may then use the service name to obtain the IBE public parameter information from the appropriate host.

These aspects of applicants' invention are set forth in applicants' claims. In particular, independent claim 1 is directed to a method in which a service name generation rule is used at a sender to generate a service name for a host based on the IBE public key of a desired recipient. According to claim 1, the service name is used to obtain the IBE public parameter information associated with the recipient for the sender from the IBE public parameter host over a network. Claim 1 also specifies how the sender uses the IBE public parameter information obtained from the IBE public parameter host and the IBE public key of the recipient to encrypt a message for the recipient.

The prior art that was relied upon in the Office Action does not show or suggest the method steps of claim 1.

The rejection of claim 1 that was made in the Office Action was a §103 rejection based on a proposed four-way combination of AAPA, Mont, Smith, and Lee. The primary

reference -- AAPA -- is the description of IBE systems that applicants included in the background section of the present patent application. However, AAPA does not show or suggest the method steps of claim 1, as conceded in the Office Action (see, e.g., page 4, lines 10-16). For example, AAPA does not disclose applicants' claimed step of "at the sender, using a service name generation rule to generate the service name of the host based on the IBE public key of the recipient." This is not surprising, because AAPA does not even show or suggest an IBE arrangement using IBE public parameter hosts with service names to store IBE public parameters.

To make up for the deficiencies in AAPA, the Office Action relies on the secondary references of Mont, Smith, and Lee.

The main focus of the Mont article is on a "Time Vault" service in which a document can be encrypted so that it is not accessible until a particular time. The time-encrypted document can be distributed widely, because it will be secure until the particular point in time has been reached. The Time Vault service is unlike applicants' claimed method, because Time Vault documents are not encrypted for a particular recipient. The Time Vault service therefore does not show or suggest using the IBE public key of a recipient to encrypt a message for a recipient or the other aspects of claim 1.

A secondary focus in Mont is the description of a conventional IBE system. This description, which is presented at pages 8-10 of Mont, is the portion of Mont relied upon in the Office Action (see page 3 of the Office Action, citing pages 9 and 11 of Mont).

In the conventional IBE system described in Mont, a sender, Alice, wants to send an encrypted message to a recipient Bob. A trust authority (TA) (private key generator) in this system generates decryption keys (i.e., a private key for Bob) and a public detail (i.e., IBE public parameter information that Alice will need to encrypt the message to Bob). In this conventional IBE system, there is only a single TA and a single public detail. Accordingly, the issues associated with handling multiple sets of IBE public parameter information are not addressed.

In particular, there is no mention in the description of Mont's conventional IBE system of any potential difficulties associated with locating the appropriate IBE public parameter information for Alice to use in encrypting the message to Bob. In FIG. 2, Mont states that the public detail is "well known or available from reliable source." Under item 2 at the bottom of page 9, Mont states that Alice trusts the TA and retrieves the public detail from the TA site. Mont does not even recognize that different sets of recipients might have different public

details, let alone show or suggest any techniques for Alice to determine how to locate the appropriate public detail using a service name generation rule. Moreover, Mont makes no suggestion that Alice should use Bob's IBE public key when retrieving the public detail.

Smith and Lee fail to make up for the deficiencies of AAPA and Mont. Neither of these references makes any mention of identity-based encryption, let alone techniques that would address the problems associated with obtaining the correct IBE public parameter information needed to encrypt a message.

In the Smith system, a sender directs a delivery server to contact a certificate authority to obtain the PKE public key of a recipient. The certificate authority provides the PKE public key of the recipient to the delivery server. The delivery server then provides the PKE public key of the recipient to the sender. The sender uses one of several different potential schemes to encrypt a document for the recipient using the PKE public key provided by the delivery server. The PKE private key of the recipient is used to access the encrypted document.

PKE-based systems such as the Smith system have a number of disadvantages related to looking up PKE public keys. With IBE encryption schemes, in contrast, it is generally not necessary to look up a given recipient's public key. IBE

systems use identity-based public keys, so the public key of a recipient can be determined, for example, by ascertaining the email address of the recipient.

Smith does not disclose or suggest using IBE techniques to convey the Smith document securely. Smith therefore does not provide any insight into how to locate appropriate IBE public parameter information for encrypting a message for a recipient, let alone disclose or suggest using a service name generation rule to generate a service name of an IBE public parameter host as set forth in claim 1.

Lee does not make up for the shortcomings of AAPA, Mont, and Smith. Lee's system contacts mail servers to check the validity of email addresses. Lee fails to show or suggest that the mail servers should be used to store IBE public parameter information or any other encryption information. Lee also fails to show or suggest using a service generation rule to generate the service name of a IBE public parameter host based on the IBE public key of a recipient.

There is therefore nothing in the cited references that shows or suggests the method steps of claim 1. In particular, none of the references discloses the claim 1 method step of "at the sender, using a service name generation rule to generate the service name of the host based on the IBE public key of the recipient." This feature is missing from each of the

references. Accordingly, even if the references were to be combined, the combination would still fail to disclose all of the features of claim 1.

Moreover, the Office Action has not provided a proper prior art motivation for making the proposed combination under 35 U.S.C. §103(a).

For example, it was stated that it would be obvious to combine AAPA and Mont because the "public detail/parameter is used to provide functionality of a trusted party so that the recipient can trust that the message came from an authentic source" (Office Action, page 3). This is incorrect. The public detail in Mont is not used so that the recipient can trust that an encrypted message comes from an authentic source. Bob must trust the TA in order to receive Bob's private key for decrypting the message. Because the public detail is not used so that Bob can trust the TA, the alleged motivation for combining AAPA and Mont is based on false premise.

AAPA describes how the recipient can provide the IBE public parameter information to the sender directly. If this approach were to be modified to follow Mont's suggestion of obtaining the public detail from the TA, the AAPA system would only be able to support a single set of IBE public parameter information. This would significantly detract from the capabilities of the AAPA system, which teaches away from making

the proposed modification. Because the reason given in the Office Action for combining Mont and AAPA is based on an incorrect assumption and because the prior art teaches away from combining Mont and AAPA, it would not be obvious to combine Mont and AAPA under 35 U.S.C. § 103(a).

With respect to Smith, the Office Action suggests that the sender in an IBE system could request an IBE public key from a delivery server to use to encrypt messages to the recipient. (Office Action, page 4). This is unconvincing. An important advantage of using IBE techniques over PKE techniques of the type described in Smith is that it is not necessary to look up the public key of the recipient. Rather, the public key of the recipient can be generated from known rules without any lookup operation. Forcing a sender to contact a server to obtain the IBE public key of the recipient would therefore negate a significant advantage of the IBE approach. The prior art therefore teaches away from combining Smith's public key lookup arrangement with the IBE systems of AAPA and Mont.

The Office Action further suggests that Smith should be combined with AAPA and Mont because "using the public key of trusted authority to encrypt messages increases the authenticity and security of the message" (Office Action, page 4). However, if AAPA and Mont were modified to encrypt messages for the recipient using a public key of a trusted authority, only the

trusted authority (who has a corresponding private key) would be able to decrypt the messages. This would prevent the desired recipient of the message from accessing its contents, which also teaches away from modifying AAPA and Mont according to Smith.

With respect to Lee, the Office Action suggests that it would be obvious to combine Lee with AAPA, Mont, and Smith, because this would allow a sender to check whether the address for the intended recipient exists and whether the address and domains are correct. However, for this arrangement to work, the email server name that is generated from the email address would need to correspond to mail server, not an IBE public parameter host. Providing the functionality that the Office Action says is desirable would therefore result in a system that would not satisfy its intended purpose of providing appropriate IBE public parameter information to the sender. This teaches away from using Lee's email server lookup technique in combination with AAPA, Mont, and Smith.

Even if the AAPA, Month, Smith and Lee references were to be combined as urged in the Office Action, this four-way combination of references would still fail to disclose the steps of claim 1. Features such as the use of a service name generation rule to generate the service name of the IBE public parameter host are absent from each of the references individually, so the combination would still not have all of the

features of claim 1. Moreover, the Office Action has not presented a sufficient prior art motivation under 35 U.S.C. § 103(a) for making the proposed combination of AAPA, Mont, Smith, and Lee. As has been demonstrated, the prior art teaches away from combining these references.

For each of these reasons, claim 1 is allowable over AAPA, Mont, Smith, and Lee. Claims 2-24 depend from claim 1 and are allowable because claim 1 is allowable. This application is therefore in condition for allowance. Reconsideration of this patent application and allowance are respectfully requested.

Respectfully submitted,

G. Victor Treyz 2/8/05

G. Victor Treyz
Reg. No. 36,294
Attorney for Applicants
Customer No. 36532